PATENT ABSTRACTS OF JAPAN

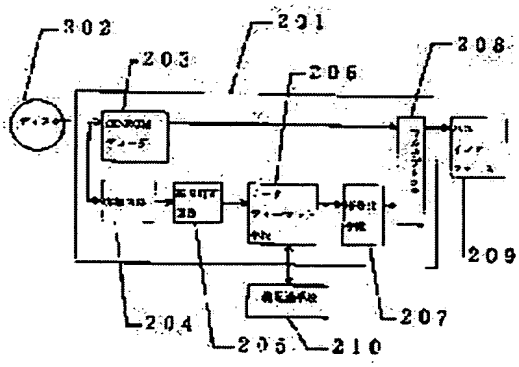
(11)Publication number : **09-320192**
(43)Date of publication of application : **12.12.1997**

(51)Int.CI. G11B 20/10
G06F 3/06
G06F 12/14
G09C 1/00
H04L 9/08

(21)Application number : **08-133523**
(22)Date of filing : **28.05.1996**

(71)Applicant : **MITSUBISHI ELECTRIC CORP**
(72)Inventor : **SAKAI YASUYUKI**
CHIKASAWA TAKESHI
YAMAGISHI ATSUHIRO
TAKEDA EISAKU
OGAWA MASAHARU

(54) METHOD AND DEVICE FOR PROTECTING COPYRIGHT



(57)Abstract:
PROBLEM TO BE SOLVED: To prevent the data from being improperly copied by adding to the digital data copy control information, discriminative information, etc., of ciphering algorithm.
SOLUTION: The digital data error corrected by an error correction circuit 205 are inputted to a data format means 206, and a header for protecting copyright is added to the top of the data. The header is constituted of ciphering start information, a ciphering key, a unit of ciphering, the copy control information showing the information on whether or not the copy of the data is allowed and the discriminative information of the used ciphering algorithm. The ciphering key is a random number information generated by a key delivery means 210, and the header itself contains also another random number information, shared with procedure by a Diffy-Helman type key delivery system as key information. The inproper copy of the data is prevented since the data added with the header are ciphering processed when the copy is not allowed.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－320192

(43)公開日　平成９年(1997)12月12日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｇ１１Ｂ	20/10		7736－5D	Ｇ１１Ｂ	20/10	Ｈ
Ｇ０６Ｆ	3/06	３０４		Ｇ０６Ｆ	3/06	３０４Ｍ
	12/14	３１０			12/14	３１０Ｋ
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ａ
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ａ

審査請求　未請求　請求項の数３　ＯＬ　（全６頁）

(21)出願番号　特願平8－133523

(22)出願日　平成８年(1996)５月28日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　酒井　康行
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(72)発明者　近澤　武
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

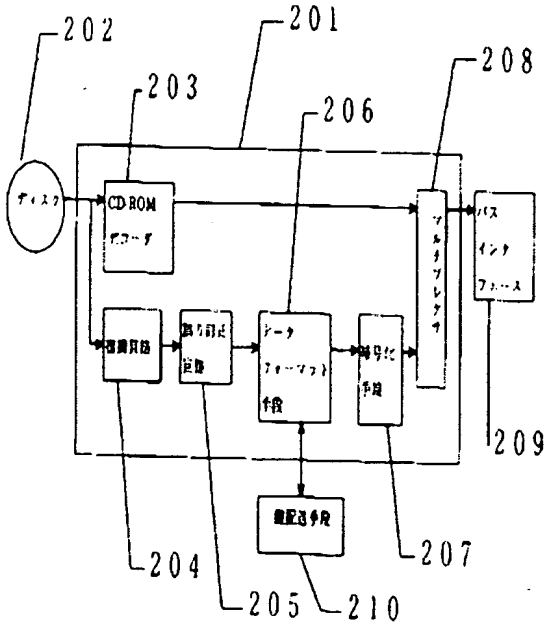
(72)発明者　山岸　篤弘
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(74)代理人　弁理士　宮田　金雄　（外３名）

最終頁に続く

(54)【発明の名称】　著作権保護方法及び装置

(57)【要約】
【課題】　著作者の権利を保護できる著作権保護方法及び装置を得ることを課題とする。
【解決手段】　ディスクから読み出されたディジタル情報に、暗号化開始情報、暗号化鍵、暗号化の単位、データの複製を許可するか否かの情報を示す複製管理情報、及び使用する暗号化アルゴリズムの識別情報を付加するデータフォーマット手段２０６と、前記ディジタル情報を暗号化する暗号化手段とを備えた。



【特許請求の範囲】
【請求項１】　ディジタル情報に、暗号化開始情報、暗号化鍵、暗号化の単位、データの複製を許可するか否かの情報を示す複製管理情報、及び、使用する暗号化アルゴリズムの識別情報を付加することを特徴とする著作権保護方法。
【請求項２】　ディジタル情報に、暗号化開始情報、暗号化鍵、暗号化の単位、データの複製を許可するか否かの情報を示す複製管理情報、及び、使用する暗号化アルゴリズムの識別情報を付加するデータフォーマット手段と、前記ディジタル情報を暗号化する暗号化手段とを備えたことを特徴とする著作権保護装置。
【請求項３】　暗号化ディジタル情報に付加された、暗号化開始情報、暗号化鍵、暗号化の単位、データの複製を許可するか否かの情報を示す複製管理情報、及び、使用する暗号化アルゴリズムの識別情報を復号するデータフォーマット手段と、このデータフォーマット手段により復号された情報に基づいて前記暗号化ディジタル情報を復号する復号手段とを備えたことを特徴とする著作権保護装置。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データの不正な複製を防ぐことができる著作権保護方法及び装置に関する。
【０００２】
【従来の技術】従来のＤＶＤ（Ｄｉｇｉｔａｌ Ｖｉｄｅｏ Ｄｉｓｃ）を再生する装置およびそこで使用されているデータフォーマットについて説明する。
【０００３】図６は、ＤＶＤを再生する装置で用いられている従来のデータフォーマットを説明する図である。図において、６０１はデータフォーマット、６０２はヘッダー、６０３はデータ、６０４はテーラーである。ヘッダー６０２には、著作権保護に関する情報が書き込まれている。
【０００４】図７は、ＤＶＤを再生するための従来の光ディスクシステムである。図において７０１はＤＶＤドライブ、７０２はＤＶＤ又はＣＤ－ＲＯＭのディスク、７０３はＣＤ－ＲＯＭデコーダ、７０４は復調回路、７０５は誤り訂正回路、７０６はマルチプレクサ、７０７はバスインタフェースである。ＤＶＤドライブ７０１はＤＶＤとＣＤ－ＲＯＭの両方のディスクを再生できるように構成されている。次に動作を説明する。ディスク７０２から読み出されたデータは、ＣＤ－ＲＯＭデコーダ７０３および復調回路７０４に入力される。ＣＤ－ＲＯＭデコーダ７０３ではＣＤ－ＲＯＭの場合の復調、誤り訂正が行われる。復調回路７０４ではディスク７０２から読み出された信号をディジタルデータに復調する。復調されたデータは、誤り訂正回路７０５に入力され、ＤＶＤフォーマットのデータの誤り訂正を行う。マルチプレクサ７０６では、ディスク７０２がＤＶＤ、ＣＤ－ＲＯＭのいずれであるかに応じてデータを選択し、バスインタフェース７０７に出力する。
【０００５】
【発明が解決しようとする課題】従来の光ディスクシステムは、ディスクに記録されているディジタルデータを何ら加工せず、記録されているままに再生していた。そのため、ディスクに記録されているデータの複製を作ることが容易であり、データの著作者の権利を保護することが困難であるという課題があった。
【０００６】本発明の目的は、係る課題を解決するためになされたもので、データの複製を作ることが困難で、著作者の権利を保護することができる著作権保護方法及び装置を得ることにある。
【０００７】
【課題を解決するための手段】本発明の請求項１に係る著作権保護方法は、ディジタル情報に、暗号化開始情報と、暗号化鍵と、暗号化の単位と、データの複製を許可するか否かの情報を示す複製管理情報と、使用する暗号化アルゴリズムの識別情報とを付加するものである。
【０００８】本発明の請求項２に係る著作権保護装置は、ディジタル情報に、暗号化開始情報、暗号化鍵、暗号化の単位、データの複製を許可するか否かの情報を示す複製管理情報、及び、使用する暗号化アルゴリズムの識別情報を付加するデータフォーマット手段と、前記ディジタル情報を暗号化する暗号化手段とを備えたものである。
【０００９】本発明の請求項３に係る著作権保護装置は、暗号化ディジタル情報に付加された、暗号化開始情報、暗号化鍵、暗号化の単位、データの複製を許可するか否かの情報を示す複製管理情報、及び、使用する暗号化アルゴリズムの識別情報を復号するデータフォーマット手段と、このデータフォーマット手段により復号された情報に基づいて前記暗号化ディジタル情報を復号する復号手段とを備えたものである。
【００１０】
【発明の実施の形態】
実施の形態１．本発明による著作権保護方法の一実施の形態を図１に基づいて説明する。図１は、本実施の形態によるデータフォーマットを説明する図である。図において、１０１はデータフォーマット、１０２はヘッダー、１０３はデータ、１０４はテーラーである。
【００１１】次に動作を説明する。データ１０３はディスクに記録されていたデータであり、データ１０３の先頭に著作権保護のためのヘッダー１０２を付加する。ヘッダー１０２は次の情報から構成される。第１は暗号化スタート情報で、この情報以降のデータが暗号化されていることを示す。第２は暗号化鍵である。第３は暗号化の単位で、暗号化する情報の単位のバイト数を示す。第４は複製管理情報で、データの複製を許可するか否かの

情報を示す。データの複製を許可しないならば、データを暗号化することにより秘匿することができる。第５は暗号化アルゴリズムを示し、暗号化処理に用いる暗号アルゴリズムを、複数の中から選択できる。テーラー１０４はデータの終了を示す。このヘッダー１０２を付加することにより、データの著作者が複製を許可しない場合は、データを暗号化することができ、データの不正な複製を防ぐことができる。

【００１２】実施の形態２．本発明による著作権保護装置の一実施の形態を、図２に基づいて説明する。図２は、本実施の形態による著作権保護装置の構成図である。図において、２０１はＤＶＤドライブ、２０２はＤＶＤ、又はＣＤ－ＲＯＭのディスク、２０３はＣＤ－ＲＯＭデコーダ、２０４は復調回路、２０５は誤り訂正回路、２０６はデータフォーマット手段、２０７は暗号化手段、２０８はマルチプレクサ、２０９はバスインタフェース．２１０は鍵配送手段である。

【００１３】次に動作を説明する。ＤＶＤドライブ２０１は、ＤＶＤ、ＣＤ－ＲＯＭいずれのディスクも再生できるように構成されている。ディスク２０２から読み出されたデータは、ＣＤ－ＲＯＭデコーダ２０３および復調回路２０４に入力される。ＣＤ－ＲＯＭデコーダ２０３ではＣＤ－ＲＯＭの場合の復調、誤り訂正が行われる。復調回路２０４ではディスク２０２から読み出された信号をディジタルデータに復調する。復調されたデータは、誤り訂正回路２０５に入力され、ＤＶＤフォーマットのデータの誤り訂正を行う。誤り訂正されたデータは、データフォーマット手段２０６に入力され、前記ヘッダー１０２およびテーラー１０４が付加される。次に暗号化手段２０７に入力され、ヘッダー１０２の情報に基づいて暗号化処理が行われる。マルチプレクサ２０８では、ディスク２０２がＤＶＤ、ＣＤ－ＲＯＭのいずれであるかに応じてデータを選択し、バスインタフェース２０９にデータを出力する。データフォーマット手段２０６において付加される暗号化鍵は、鍵配送手段２１０により生成される乱数情報であり、ヘッダー１０２自身もディフィーヘルマン型鍵配送方式による手順により共有化される別の乱数情報を鍵情報として暗号化される。ディフィーヘルマン型鍵配送方式は公知の技術であり、例えば、池野、小山著、電子情報通信学会編、「現代暗号理論」に記載されている。本実施の形態の著作権保護装置は、データフォーマット手段２０６と暗号化手段２０７と鍵配送手段２１０とを備えていることにより、バスインタフェース２０９に出力されるデータには、著作者の意図により暗号化を施すことができるので、データの不正な複製を防ぎ、著作者の権利を保護することができる。

【００１４】実施の形態３．本発明による著作権保護装置の一実施の形態を、図３に基づいて説明する。図３は、本実施の形態による著作権保護装置の構成図である。図において、３０１はＤＶＤドライブ、３０２はＤＶＤ又はＣＤ－ＲＯＭのディスク、３０３はＣＤ－ＲＯＭデコーダ、３０４は復調回路、３０５は誤り訂正回路、３０６はマルチプレクサ、３０７はデータフォーマット手段、３０８は暗号化手段、３０９はバスインタフェース、３１０は鍵配送手段である。

【００１５】次に動作を説明する。ＤＶＤドライブ３０１は、ＤＶＤ、ＣＤ－ＲＯＭいずれのドライブも再生できるように構成されている。ディスク３０２から読み出されたデータは、ＣＤ－ＲＯＭデコーダ３０３および復調回路３０４に入力される。ＣＤ－ＲＯＭデコーダ３０３ではＣＤ－ＲＯＭの場合の復調、誤り訂正が行われる。復調回路３０４ではディスク３０２から読み出された信号をディジタルデータに復調する。復調されたデータは、誤り訂正回路３０５に入力され、ＤＶＤフォーマットのデータの誤り訂正を行う。マルチプレクサ３０６では、ディスク３０２がＤＶＤ、ＣＤ－ＲＯＭのいずれであるかに応じてデータを選択する。次に、データは、データフォーマット手段３０７に入力され、前記ヘッダー１０２およびテーラー１０４が付加される。次に暗号化手段３０８に入力され、ヘッダー１０２の情報に基づいて暗号化処理が行われる。暗号化されたデータは、バスインタフェース３０９に出力される。データフォーマット手段３０７において付加される暗号化鍵は、鍵配送手段３１０により生成された乱数情報であり、ヘッダー１０２自身も、ディフィーヘルマン型鍵配送方式による手順で共有化される別の乱数情報を鍵情報として暗号化される。本実施の形態の著作権保護装置は、データフォーマット手段３０７と暗号化手段３０８と鍵配送手段３１０とを備えていることにより、バスインタフェース３０９に出力されるデータには、著作者の意図により暗号化を施すことができるので、データの不正な複製を防ぎ、著作者の権利を保護することができる。

【００１６】実施の形態４．本発明による著作権保護装置の一実施の形態を、図４に基づいて説明する。図４は、本実施の形態による著作権保護装置の構成図で、ディスクに記録されている映像等をディスプレイに表示する構成を示している。図において、４０１はバスインタフェース、４０２はコンピュータ、４０３はＡＶボード、４０４はデータフォーマット手段、４０５は復号手段、４０６はビデオ回路、４０７はディスプレイ、４０８は鍵配送手段である。

【００１７】次に動作を説明する。バスインタフェース４０１には、前記発明の実施の形態２および３で説明した、ヘッダー付の暗号化されたデータが入力される。データはコンピュータ４０２を介してＡＶボード４０３に入力される。ＡＶボード４０３内では、まずデータフォーマット手段４０４にデータは入力される。ここでは、ディフィーヘルマン型鍵配送方式により共有化された鍵情報により前記ヘッダー１０２を復号し、前記ヘッダー

１０２に含まれる情報に基づいて、暗号アルゴリズムの種類、暗号化の単位、暗号化鍵等の情報を、復号手段４０５に送信する。これに基づき復号手段４０５では、データの復号処理を行う。復号されたデータは、ビデオ回路４０６から、ディスプレイ４０７に表示される。データフォーマット手段４０４において出力される暗号化鍵は、鍵配送手段４０８により、ディフィーヘルマン型鍵配送方式による手順で共有化された別の鍵情報により暗号化することで暗号化されたヘッダー１０２に含まれる。本実施の形態の著作権保護装置は、データフォーマット手段４０４と復号手段４０５と鍵配送手段４０８とを備えていることにより、暗号化鍵を共有しない場合はデータを復号することができないので、データの不正にディスプレイ表示することを防ぐことができ、著作者の権利を保護することができる。

【００１８】実施の形態５．本発明による著作権保護装置の一実施の形態を、図５に基づいて説明する。図５は、本実施の形態による著作権保護装置の構成図で、ディスクに記録されている映像等をディスプレイに表示する構成を示している。図において、５０１はバスインタフェース、５０２はコンピュータ、５０３はハードディスク、５０４はデータフォーマット手段、５０５は復号手段、５０６はＡＶボード、５０７はビデオ回路、５０８はディスプレイ、５０９は鍵配送手段である。

【００１９】次に動作を説明する。バスインタフェース５０１には、前記発明の実施の形態２および３で説明した、ヘッダー付きの暗号化されたデータが入力される。データはコンピュータ５０２内に入力される。コンピュータ５０２内では次の動作をする。ハードディスク５０３内にデータを保存する場合、暗号化されているデータを復号するには、データフォーマット手段５０４、復号手段５０５を介さなければならない。つまり、鍵配送、例えば前記のディフィーヘルマン型鍵配送により正しい暗号化鍵を伝送されなければ、暗号を解くことはできない。したがって、不正な複製を防止することができる。データをディスプレイに表示する際にも、データフォーマット手段５０４、復号手段５０５により復号を行う。データフォーマット手段５０４において出力される暗号化鍵は、鍵配送手段５０９により、ディフィーヘルマン型鍵配送方式による手順で共有化された別の鍵情報により暗号化することで暗号化されたヘッダー１０２に含まれる。本実施の形態の著作権保護装置は、データフォーマット手段５０４と復号手段５０５と鍵配送手段５０９とを備えていることにより、暗号化鍵を共有しない場合はデータを復号することができないので、データの不正にハードディスクに保存したり、ディスプレイに表示することを防ぐことができ、著作者の権利を保護することができる。

【００２０】実施の形態６．前記実施の形態２、３、４および５では、暗号化鍵を共有するための秘密情報はあらかじめ装置内に保持していたが、秘密情報を外部から与えるように構成することも可能である。

【００２１】実施の形態７．前記実施の形態３では、データフォーマット手段は、ＤＶＤドライブ３０１より出力されたディジタル情報を入力して処理したが、ＤＶＤドライブ３０１でなくても良く、ディジタル情報を出力する装置であれば良い。

【００２２】

【発明の効果】以上のように本発明による著作権保護方法及び装置は、データの不正な再生、複製、およびディスプレイ表示を防ぐことができ、著作者の権利を保護することができる効果がある。

【図面の簡単な説明】

【図１】　本発明の実施の形態１の著作権保護方法を説明する図である。

【図２】　本発明の実施の形態２の著作権保護装置の構成図である。

【図３】　本発明の実施の形態３の著作権保護装置の構成図である。

【図４】　本発明の実施の形態４の著作権保護装置の構成図である。

【図５】　本発明の実施の形態５の著作権保護装置の構成図である。

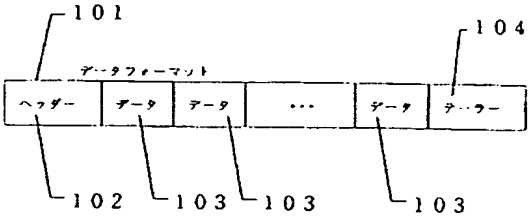
【図６】　従来のデータフォーマットを説明する図である。

【図７】　従来の光ディスクシステムの構成図である。

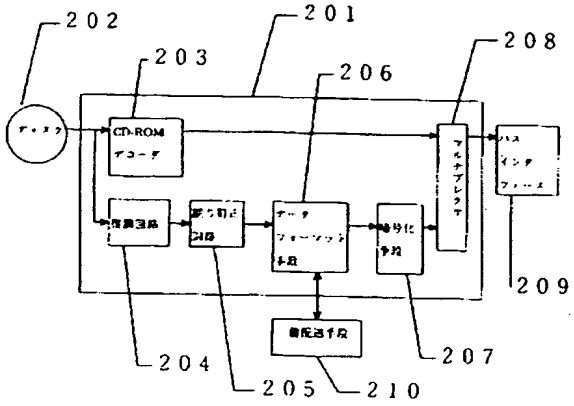
【符号の説明】

１０１　データフォーマット、１０２　ヘッダー、１０３　データ、１０４テーラー、２０１　ＤＶＤドライブ、２０２　ディスク、２０３　ＣＤ－ＲＯＭデコーダ、２０４　復調回路、２０５　誤り訂正回路、２０６　データフォーマット手段、２０７　暗号化手段、２０８　マルチプレクサ、２０９　バスインタフェース、２１０　鍵配送手段。

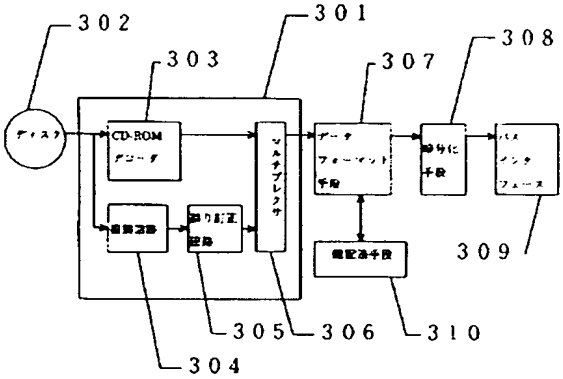
【図１】



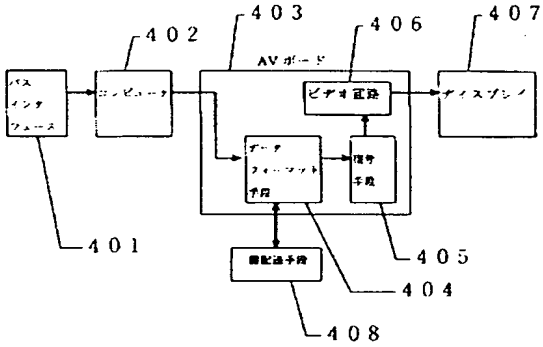
【図２】



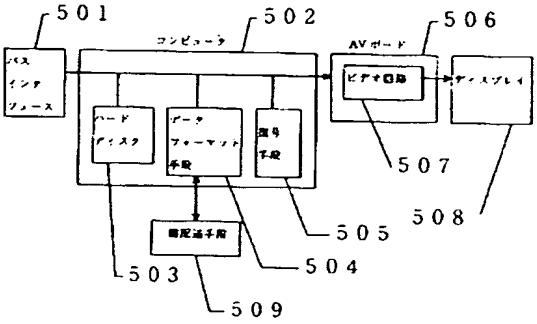
【図３】



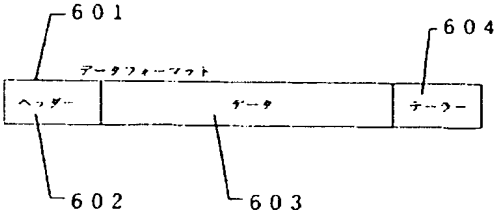
【図４】



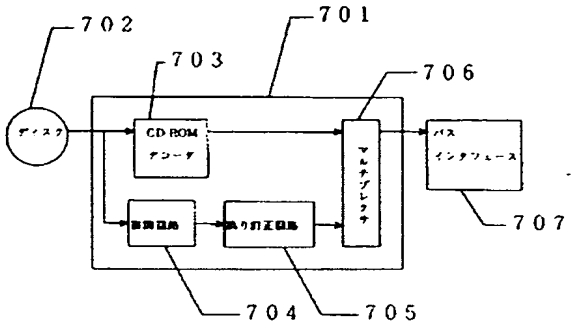
【図５】



【図６】



【図７】



フロントページの続き

(72)発明者　竹田　栄作
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(72)発明者　小川　雅春
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内